AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, David Albers, a task force officer (TFO) with the Federal Bureau of Investigation (FBI), Kansas City, Missouri, being duly sworn, depose and state as follows:

1. As a TFO, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. At all times throughout this affidavit I use the term "child pornography" merely as shorthand to refer to visual depictions of actual minors engaged in sexually explicit conduct. I use the terms "visual depiction," "minor," and "sexually explicit conduct" as those terms are defined in 18 U.S.C. § 2256.

2. I am a twenty-one year veteran of the Kansas City, Missouri Police Department. I have investigated crimes against children for approximately thirteen years. I was assigned specifically to the FBI Child Exploitation Task Force over six years ago to investigate computer crimes involving violations against children. I have gained expertise in the conduct of such investigations through training in seminars, classes, and everyday work related to conducting these types of investigations. I have attended training such as the annual Crimes Against Children Conference and Innocent Images training provided by the FBI. I have assisted in the investigation of hundreds of child pornography cases. During that time, I have had to view thousands of images of child pornography. I have previously applied the federal definition of child pornography used in this affidavit to dozens of search warrant applications and in dozens of grand jury presentations.

3. I am investigating activities occurring via a TracFone cellular phone number (816) 756-7331 (also referred to herein as **SUBJECT CELL PHONE**) utilized by **Thomas ANDRIES** (hereinafter **ANDRIES**). As will be shown below, there is probable cause to believe **ANDRIES** has transmitted child pornography, in violation of Title 18, United States Code, Section 2252. I am submitting this affidavit in support of two separate search warrants authorizing searches of the

following:

a. **ANDRIES'S** residence (further described in **Attachment A** to Search Warrant **19-SW-00141-MJW)** for a cell phone with phone number (816) 756-7331; and

b. **ANDRIES'S** person (further described in **Attachment A** to Search Warrant **19-SW-00148-MJW**) for a cell phone with phone number (816) 756-7331.

This application is also to seize and search the **SUBJECT CELL PHONE** where the items specified in **Attachment B** to each warrant may be found, and to seize all items listed in **Attachment B** to each warrant as contraband, instrumentalities, fruits, and evidence of crime.

4. The statements in this affidavit are based on information received from SA Dustin Grant, FBI, Salt Lake City Division, from SA Mike Daniels, FBI Kansas City Division, and my investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe contraband, evidence, fruits, and instrumentalities of the violation of Title 18, United States Code, Section 2252 are presently located on the **SUBJECT CELL PHONE** utilized by **ANDRIES**.

BACKGROUND OF THE INVESTIGATION

5. On February 12, 2019, a FBI Task Force Officer (TFO) in Salt Lake City, posing as a 13 year old female in an online undercover capacity, engaged in a conversation with an individual on Kik[1] with the username of "umbrasval", profile name **Thomas ANDRIES**. During

1 Kik is a mobile messaging application for use on computers and mobile electronic devices. The

the communication, **ANDRIES** expressed an interest in engaging in sexual activity with the purported 13 year old and asked for nude photos. **ANDRIES** sent images and videos of prepubescent children engaging in sexually explicit activities to the TFO. **ANDRIES** also sent a face photo, which appeared to match the individual in the Kik profile photo.

6. On February 13, 2019, an administrative subpoena was sent to Kik Interactive, Inc., requesting subscriber information for the username umbrasval. On February 15, 2019, in response to the subpoena, Kik indicated the subscriber was **Thomas ANDRIES**, email address of dhgwckedtr1cks@gmail.com, and cell phone at time of registration on October 5, 2018 being a Samsung SM-S727VL. Kik also provided an IP address connection log. In particular, on February 12, 2019, at 23:51 UTC, **ANDRIES** (Kik user umbrasval) connected to Kik via the IP address of 174.254.129.155. Notably, on February 12, 2019, at 23:56 UTC, **ANDRIES** was engaging in the conversation with the undercover TFO described in paragraph 5 above. Additionally, the IP address connection log provided by Kik also established that **ANDRIES** accessed Kik via IP address 97.32.5.172 on February 13, 2019, at 14:10 CST; 174.254.129.155 on February 14, 2019, at 18:38 CST (the same as that noted above for February 12, 2019); and 174.254.132.65 on February 15, 2019, at 9:06 CST. All three IP addresses returned to Verizon.

7. On March 7, 2019, a Missouri driver's license photo was requested for **ANDRIES** from the Missouri Department of Revenue. The photo matched the Kik profile photo and face photo received by the undercover TFO. **ANDRIES'S** current home address was listed as **535 South Glenwood Street, Independence, Missouri**.

---

application can be used for text communication as well as sending and receiving photos and videos in electronic format.

8. Open source Internet searches were conducted to further connect **ANDRIES** to the email account dhgwckedtr1cks@gmail.com. Associated with that email address were Skype, Tumblr, LinkedIn, and Instagram accounts all with the username of **Thomas ANDRIES** and profile photos matching those photos previously identified as **ANDRIES**. Additionally, **ANDRIES** posted on Facebook that he worked for Allied Universal Security Services.

9. Human Resources for Allied Universal Security Services was contacted. They advised **ANDRIES** did work for the company. His regular shift was Monday through Friday, 2:00 through 10:00pm. Comparing these times with the IP address connection logs indicated **ANDRIES** connected to Kik while at work and potentially at home. **ANDRIES** provided Allied Universal Security Services with a contact number of (816) 756-7331.

10. On March 11, 2019, an administrative subpoena was sent to Verizon requesting subscriber information for the three IP addresses noted above. On March 23, 2019, in response to the subpoena, Verizon indicated it could not provide specific subscriber information for the subject IP addresses. Verizon did provide, however, a list of multiple phone numbers that had utilized the IP addresses at the dates and times noted above. A review of the results revealed only one phone number utilized all three IP addresses at the dates and times in question. The Verizon records establish that only a cell phone with phone number (816) 756-7331 had utilized all three IP addresses during the applicable dates and times.

11. On March 25, 2019, an administrative subpoena was sent to Verizon requesting subscriber information for the cell phone number noted above. On April 11, 2019, in response to the subpoena, Verizon indicated the phone number had been resold to TracFone so no subscriber information was available.

12. From April 15 through April 16, 2019, surveillances were conducted in the vicinity of **535 South Glenwood Street, Independence, Missouri.** During that time, **ANDRIES** was observed on the front porch of the residence. Investigation has determined this address is owned by **ANDRIES'S** former sister-in-law. **ANDRIES** parked his vehicle next door in the driveway of 537 South Glenwood Street, Independence, Missouri. The residence at 537 South Glenwood Street appears to be a vacant house with boarded up windows.

13. On April 24, 2019, open source records were searched for the cell phone number (816) 756-7331. That number was connected to Facebook, Telegram, and Whatsapp accounts for **Thomas ANDRIES**.

DEFINITIONS

14. The following definitions apply to this Affidavit and **Attachment B** to this Affidavit:

a. "Child Erotica," as used herein, means materials demonstrating a sexual interest in minors, including fantasy narratives, cartoons, and books describing or alluding to sexual activity with minors, sexual aids, children's clothing catalogues, and child modeling images.

b. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

c. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).

d. "Internet Protocol address" (or simply "IP address") is a unique numeric address used by computers on the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static,

if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

e. "The Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

f. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

h. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli

drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND ON COMPUTERS, CELL PHONES, AND CHILD PORNOGRAPHY

15. Computers and cell phones basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

16. The storage capacity of the electronic storage media used in home computers and cell phones has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

17. A user can set up an online storage account from any computer or cell phone with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer or cell phone. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or cell phone in most cases.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

18. Searches and seizures of evidence from cellular phones commonly require agents to download or copy information from the cellular phone to be processed later in a laboratory or other controlled environment. This is almost always true because of the following:

a. Cellular phones can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

b. Searching cellular phones for criminal evidence can be a technical process requiring forensic tools and a properly controlled environment. The vast array of hardware, software, and applications available makes it difficult to know before a search which tool will be necessary to analyze the system and its data. The search of a cellular phone is an exacting scientific procedure, which is designed to protect

the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since digital evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

SEARCH METHODOLOGY TO BE EMPLOYED

19. The search procedure of electronic data contained in computer hardware, computer software, memory storage devices, and/or cell phones may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. examination of all of the data contained in such computer hardware, computer software, memory storage devices, and/or cell phone to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contain;

d. opening files in order to determine their contents;

e. scanning storage areas;

f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in **Attachment B**; and/or

g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in **Attachment B**.

CHARACTERISTICS COMMON TO INDIVIDUALS INVOLVED IN THE DISTRIBUTION, RECEIPT, OR POSSESSION OF CHILD PORNOGRAPHY OR IN THE CONSPIRACIES OR ATTEMPTS TO COMMIT THOSE CRIMES

20. As set forth above, probable cause exists to believe **ANDRIES** utilized the **SUBJECT CELL PHONE** to distribute and/or possess child pornography, or has conspired or attempted to commit these crimes. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals involved in such crimes:

a. Those who distribute or possess child pornography, or who conspire or attempt to commit these crimes may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Those who distribute or possess child pornography, or who attempt or conspire to commit these crimes may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Such individuals often times use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Those who distribute or possess child pornography, or who attempt or conspire to commit these crimes often possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, videotapes, magazines, negatives, photographs, correspondences, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. **These individuals typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.**

d. Likewise, those who distribute or possess child pornography, or who attempt or conspire to commit these crimes often maintain their collections that are in a digital

or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. **These collections are often maintained for several years and are kept close by, usually at the individual's residence, to enable the collector to view the collection, which is valued highly.**

e. Those who distribute or possess child pornography, or who attempt or conspire to commit these crimes also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individual with whom they have been in contact and who share the same interests in child pornography.

f. **Those who distribute or possess child pornography, or who attempt or conspire to commit these crimes prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.**

21. Based on my training and experience as a law enforcement officer, as well as my experience personally using and owning cell phones, I know that individuals who use cell phones most often keep them on their persons and in their residences.

a. The person of **Thomas ANDRIES**, with a date of birth of February 26, 1990, is described as a white male with brown hair and blue eyes, who wears glasses and has facial hair, and who is approximately six foot one inch tall and 160 pounds, and resides at **535 South Glenwood Street, Independence, Missouri.** (Search Warrant **19-SW-00148-MJW**)

b. The residence at **535 South Glenwood Street, Independence, Missouri**, is a gray, single story home with white trim and a white railing around the front porch. The numbers "535" are located on the mailbox, on a support post on the front porch, and vertically next to the front door. The home sits on the east side of Glenwood Street. (Search Warrant **19-SW-00141-MJW**).

CONCLUSION

22. Based on the aforementioned factual information, your Affiant respectfully submits there is probable cause to believe **ANDRIES**, who utilizes the **SUBJECT CELL PHONE**, is involved in distributing and/or possessing child pornography. Your Affiant respectfully submits there is probable cause to believe **ANDRIES**, utilizing the **SUBJECT CELL PHONE**, has violated 18 U.S.C. § 2252. There is probable cause to believe that the **SUBJECT CELL PHONE** can be located on **ANDRIES'S** person and at **535 South Glenwood Street, Independence, Missouri**. Additionally, there is probable cause to believe evidence of the commission of criminal offenses, namely, violations of 18 U.S.C. § 2252 (distribution and possession of child pornography), is located in the **SUBJECT CELL PHONE**, and this evidence, listed in **Attachment B** to this affidavit, which is incorporated herein by reference, is contraband, the fruits of crime, or things otherwise criminally possessed, or property which is or has been used as the means of committing the foregoing offenses.

23. Your Affiant, therefore, respectfully requests the attached warrants be issued authorizing the search of **ANDRIES'S** person and his residence to search for the **SUBJECT CELL PHONE**, and to further search the **SUBJECT CELL PHONE** for the items listed in **Attachment B**.

David Albers
Task Force Officer
Federal Bureau of Investigation

Sworn and subscribed before me
this 14th day of May, 2019.

Honorable Sarah W. Hays
United States Magistrate Judge
Western District of Missouri.